나무위키

Tor

최근 수정 시각: 2026-08-23 13:34:45

분류: 프라이버시 | 프록시 | 다크 웹 | 2002년 출시

MLB의 프로야구단에 대한 내용은 토론토 블루제이스 문서를 참고하십시오.

편집 보호된 문서입니다. 문서의 ACL 탭을 확인하세요.

목차

1. 개요
2. 명칭
3. 상세
4. 탑재 브라우저
   4.1. 공식 클라이언트: Tor Browser
   4.2. 기타
5. 역사
6. 동작 원리
7. 보안 레벨과 브리지
   7.1. Snowflake
8. 익명성
   8.1. 사용 사례
   8.2. Operation Onymous
   8.3. 악성 코드를 이용한 추적
   8.4. 국가의 검열
   8.5. 첫 노드와 끝 노드의 장악
9. VPN과 병용
10. 억압적인 국가에서의 검열 우회
11. 국가별 릴레이
12. 검열 국가
13. 악용에 대한 프로젝트의 입장
14. 관련 문서

토어 Tor	
개발	미국 (미합중국 해군 연구소)
운영 단체	미합중국 해군 → The Tor Project[1]
분류	오버레이 네트워크
공개	2002년 9월 20일
라이센스	BSD 라이선스
Tor 중계서버(Relay) 정보	
아틀라스 https://metrics.torproject.org 글로브 https://globe.rndm.de	
링크	
[2] | | [3]	

1. 개요

Browse Privately.
Explore Freely.

은밀하게 검색하세요.
자유롭게 탐색하세요.

미국 해군 연구소에서 개발한 익명 네트워크 툴로, 미국 연방정부의 요청[4]으로 'The Tor Project'라는 민간 단체를 통해 운영 및 무료로 배포되고 있다.

2. 명칭

흔히 '토르'라고 읽지만 영어식 발음에 더 가까운 표기는 '토어'이다. 영어에서는 모음화 R 현상이 나타나 단어 끝 R 발음이 모음처럼 발음된다. 같은 단어를 남유럽에서는 또르로, 프랑스어로는 또흐로 읽을 것이다. Tor의 발음은 /tɔɹ/이다.

원래 발음과 더 가깝게 쓰려면 이렇게 쓰는 게 맞으나, /θɔɹ/로 발음되는 Thor를 토르로 표기하는 것처럼 끝의 r을 '르'로 옮긴 예외적인 경우도 많이 볼 수 있다. Petya 등의 바이러스에서는 토르라고 한다. 영미권에서도 토르, 아니면 티오알로 읽는 등 토어가 아닌 다른 발음으로 읽는 사람들이 종종 있다. CIA가 올린 유튜브 영상에서도 토르라고 쓰였다.# Tor 자체가 두문자어라서 읽는 방법이 사람들마다 많이 갈리는 듯하다.

다만 외래어 표기법에 예외가 너무나도 많기에 크게 의미는 없다. 당장 "카메라"도 영어 발음을 생각하면 "캐머러"라고 발음하는 것이 맞고, "content"는 발음상 "칸텐트"라고 하는 것이 맞지만 표준어는 발음도 다르고 마지막에 "s"가 추가된 "콘텐츠"이다. 사실 영어 단어를 보이는 대로 읽는 국가는 유럽에도 많다. "토어"와 "토르" 중 한국인 입장에서 어떤 단어가 "Tor"라는 본래 단어를 유추하기 쉬운가를 생각하면 크게 문제가 있는 표기라고 보기는 힘들다.

3. 상세

Tor는 'The Onion[5] Router'의 약칭이다. 네트워크 우회와 익명화를 위해 사용하는 툴 중 하나며, 딥 웹과 다크 웹에 이용되는 소프트웨어이다. 비슷한 것으론 Hyphanet(구 Freenet)과 I2P등이 있지만 토어는 세계적으로 가장 많이 쓰이고 있다. 많은 온라인 블랙마켓들이 .onion 도메인에 상주하고 있다. 다만 "토어 = 다크 웹"이라 착각하는 사람들도 있는데 이는 오개념이니 주의하기를 바란다. 토어 기술을 이용해 익명성이 담보된 웹 탐색을 가능하게 해주는 '브라우저' 자체는 오픈소스인 Firefox를 개조하여 사용한다.[6]

프록시 서버나 서버에 로그가 남을 가능성이 있는 VPN보다 높은 수준의 익명성이 보장된다. 토어의 트래픽은 출발지에서 각각의 공개키로 순차적으로 암호화 된다. 3개 노드를 거친다면 3중 암호화해서 보내게 된다. 최근 NSA에서 VPN을 패킷 단위로 분석할 수 있다는 발표가 있었으니 현재 정보기관으로부터 안전한 네트워크는 토어와 I2P 등의 극소수밖에 없다. 지정한 브라우저에서 송수신되는 모든 패킷을 우회시키기 때문에 많은 프록시 사이트들에 비해 우수한 안정성을 제공한다.

물론 느린 건 감안해야 한다. 느릴 수밖에 없는 게, 여러 국가의 네트워크를 경유하여 가기 때문이다. 예를 들면 자신의 컴퓨터 (한국) → 루마니아 (경유) → 러시아 연방 (경유) → 네덜란드 (경유) → 인터넷 식이다. 최종 인터넷 단계에서는 네덜란드에서 접속한 것으로 뜨게 된다. 정부가 만약 이를 역 추적하려 해도 네덜란드 → 러시아 연방 → 루마니아를 거쳐 실제 사용자의 컴퓨터까지 접근해야 하는 것이다.

토어 유저들끼리 중계 서버를 공유하여 타인의 트래픽이 자신의 컴퓨터를 거쳐갈 수 있게 할 수 있다. 이렇게 하면 토어 네트워크 속도가 더 빨라진다는 장점이 있다. 설정이 미리 되어 있으나 Configuring a Tor relay를 참고하면 좋다. 토어 네트워크가 전체적으로 빨라지는 효과가 있다. 이렇게 설정할 경우 전기/CPU 사용량이 많아진다. 사용자가 번역을 해서 도움을 줄 수도 있다.

만약 다른 프로그램에서 토어 네트워크를 사용하고 싶다면, 해당 프로그램의 프록시 설정에서 Socks5를 선택하고, 아이피를 127.0.0.1으로, 포트를 9050 또는 9150으로 설정한 뒤 토어 브라우저를 켜두면 된다. 여기서 토어 브라우저는 Whonix의 Gateway 역할을 한다고 이해하면 된다. 텔레그램, Electrum 등등 다양한 프로그램에서 토어를 활용할 수 있다.관련 글 1 관련 글 2 이외에도 Android/iOS 환경에서는 Orbot 애플리케이션을 이용해 다른 애플리케이션의 네트워크 통신이 Tor를 경유하도록 설정할 수 있다.

NSA의 XKeyscore라는 프로그램의 소스코드가 2014년에 유출되었는데 그에 따르면 토어를 사용하는 것뿐만 아니라 토어를 내려받거나 토어 공식 홈페이지에 접속하는 것만으로도 NSA 관심리스트에 오른다고 한다. 토어 네트워크를 통해 보내진 메일은 메타데이터뿐만 아니라 메일 내용까지도 저장되어 보관된다고 한다. 관련 기사 1 관련 기사 2 관련 기사 3. 이에 대해 EFF는 더 많은 평범한 사람들이 토어를 쓸수록 모두가 더 안전해진다고 하며 이용자들의 토어 사용이 위축되지 않게 장려하는 모습을 보였다. 토어 얘기는 아니었지만 암호화와 관련해서도 보안 전문가 브루스 슈나이어가 NSA같은 기관들의 대규모 무작위 감시에 대항하는 가장 좋은 방법은 더 많은 평범한 사람들이 일상에서 암호화를 이용하여 기관들이 통신들을 복호화하거나 감시하는 데 더 큰 비용이 들게 만드는 것이라 얘기한 바 있다. 예를 들어 프로톤메일 등의 PGP 방식 암호화 메일을 사용하는 방법이 있다.

안드로이드 스마트폰에서는 가디언 프로젝트(The Guardian Project)에서 만든 Orbot으로도 접속할 수 있고, 2022년에는 Tor 브라우저가 정식으로 플레이스토어에 출시되었다. (Android용으로는 Orfox도 있었으나 2019년 사라졌다.) iOS에서는 공식 애플리케이션은 없고 서드 파티 애플리케이션인 The Onion Browser를 사용하는 것이 권장되기는 하나 서드 파티 애플리케이션은 안전성과 익명성을 보장할 수 없어 주의가 필요하며, 정말 높은 익명성을 원한다면 사용을 피하는 것이 좋다.

몇몇 백신 프로그램들이 토어를 봇이나 랜섬웨어로 인식하여 실행이 안 되는 경우도 있다.

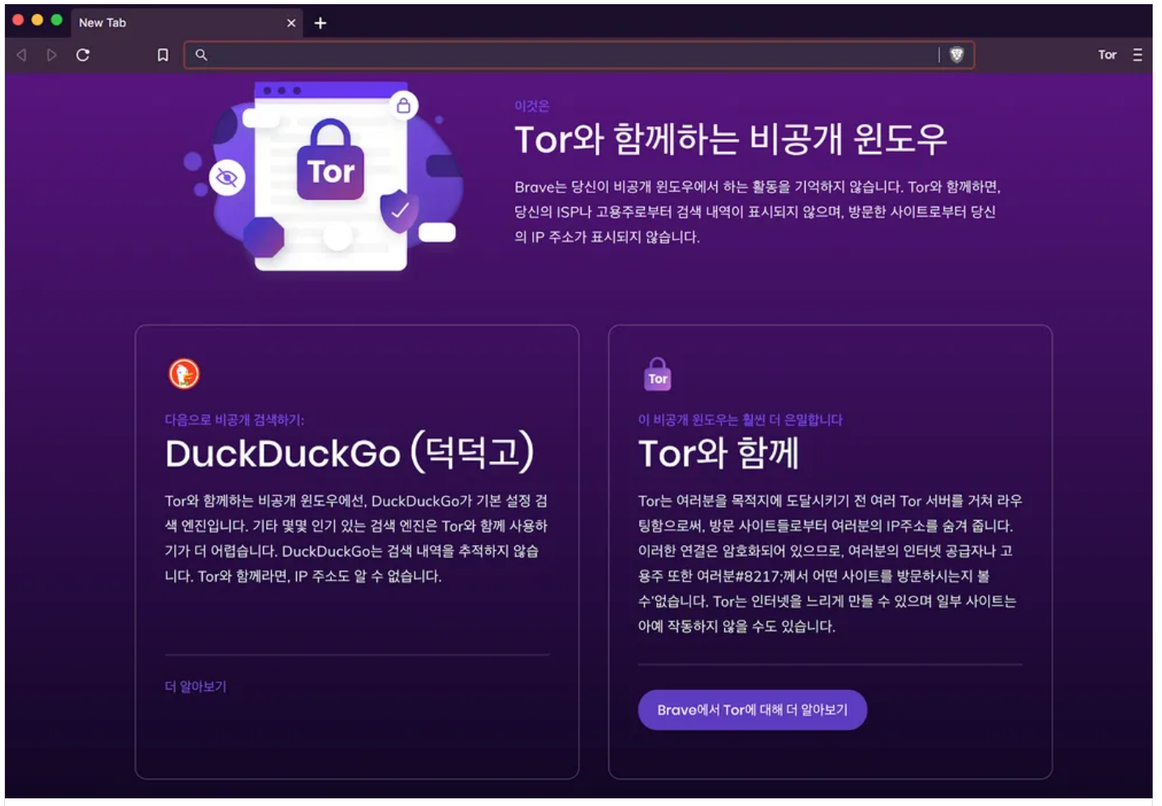
4. 탑재 브라우저

4.1. 공식 클라이언트: Tor Browser

자세한 내용은 Tor Browser 문서를 참고하십시오.

Tor를 탑재한, 프로젝트 공식 클라이언트인 Mozilla Firefox 변종 웹 브라우저.

4.2. 기타


New Tab
Tor
이것은
Tor와 함께하는 비공개 윈도우
Brave는 당신이 비공개 윈도우에서 하는 활동을 기억하지 않습니다. Tor와 함께하면, 당신의 ISP나 고용주로부터 검색 내역이 표시되지 않으며, 방문한 사이트로부터 당신의 IP 주소가 표시되지 않습니다.
다음으로 비공개 검색하기:
DuckDuckGo (덕덕고)
Tor와 함께하는 비공개 윈도우에선, DuckDuckGo가 기본 설정 검색 엔진입니다. 기타 몇몇 인기 있는 검색 엔진은 Tor와 함께 사용하기가 더 어렵습니다. DuckDuckGo는 검색 내역을 추적하지 않습니다. Tor와 함께라면, IP 주소도 알 수 없습니다.
더 알아보기
이 비공개 윈도우는 훨씬 더 은밀합니다
Tor와 함께
Tor는 여러분을 목적지에 도달시키기 전 여러 Tor 서버를 거쳐 라우팅함으로써, 방문 사이트들로부터 여러분의 IP주소를 숨겨 줍니다. 이러한 연결은 암호화되어 있으므로, 여러분의 인터넷 공급자나 고용주 또한 여러분#8217;께서 어떤 사이트를 방문하시는지 볼 수'없습니다. Tor는 인터넷을 느리게 만들 수 있으며 일부 사이트는 아예 작동하지 않을 수도 있습니다.
Brave에서 Tor에 대해 더 알아보기

Brave의 토어 기능[7]

Tor 브라우저를 제외하고도 Tor에 접속할 수 있는 브라우저가 있다. 데스크톱 버전 Brave를 사용하면 Tor 네트워크에 접속할 수 있다.[8]
Brave는 Chromium 기반 브라우저로 파이어폭스를 사용하는 Tor 브라우저와 내부 구조부터 다르다. Brave로 토어를 접속하는 유저가 매우 적은 것을 생각하면 프라이버시 면에서 Brave의 토어 기능이 아니라 토어 브라우저를 사용하는 것이 좋다. Brave를 사용하여 Tor 네트워크를 이용할 경우, Chromium 기반 브라우저를 사용하여 토어 네트워크의 IP로 접속하는 것으로 식별되므로 웹사이트/공격자 입장에서는 눈에 잘 띄게 된다. 익명성이 필요하다면 Tor 브라우저를 사용하는 것이 맞다.

Tor 브라우저는 각종 취약점이 알려질 때마다 바로 업데이트를 배포하고, 실행 전 업데이트를 설치하는 것이 기본값이라 높은 수준의 보안을 유지할 수 있다.

5. 역사

1990년대에 인터넷이 급성장하기 시작하면서, 사회는 전 세계적으로 바뀌기 시작했다. 그의 대표적인 변화가 Instant Communication 인데, 인터넷만 있으면 어디든지 소통이 가능한 장점은 인터넷 사용자를 1990년부터 2000년까지 불과 10년 만에 350만 명으로 급성장시켰다. 하지만, 인터넷은 프라이버시를 보장하지 않았기에, https와 같은 암호화 연결을 사용하지 않은 과거의 인터넷은 언제든지 기록과 트래킹이 가능했었다.

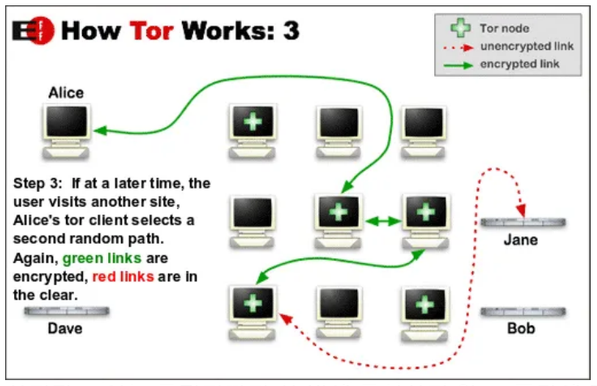
인터넷을 필요로 하는 사람 중 보안을 매우 중요시하는 집단이 있었으니, 바로 미국 정부였다. 미국 정부에 소속해 있는 미해군연구소는 Onion Routing 이라고 불리는 신기술을 개발하기 시작하였다. 이 기술은 일반 네트워크 (인터넷)이 아닌, Overlay Network 를 통하여 같은 웹페이지에 방문하더라도 완벽한 익명성을 보장하는데, 이 기술에는 치명적인 단점이 있었다. 토어 프로젝트의 공동 창설자이자 다이렉터인 로저 딩글다인(Roger Dingledine)은 2004년에 열린 컨퍼런스에서 이러한 말을 했다.

> "The United States government cannot simply run an enmity system for everybody and then use it themselves only, because then every time the connection came from it, the people will say: **"Oh, it's another CIA agent looking at my website."** if those are the only people using the network. So you NEED to have other people using the network so that they could blend together."
>
> "미국 정부는 일반 사용자들을 감시가 가능한 네트워크(인터넷)에 가둬놓고 미국 정부 자신들만 토어 네트워크를 사용할 수는 없습니다. 그렇게 되면 사이트에 토어를 이용한 연결 신호가 들어왔을 때 사람들은 **"음, CIA 요원이 내 사이트를 또 보러왔네."**라고 알 수 있게 됩니다. 그 네트워크를 쓰는 건 미국 정부뿐이니 말이죠. 따라서 미국 정부는 같은 네트워크를 이용하는 일반 사용자들이 필요합니다, 그 사람들 사이에 섞여(숨어) 들어갈 수 있게 말이죠."[9]

이렇게 토어는 대중에게 무료로 배포되었고, 현재 수십만 명의 사람들이 토어를 매우 다양한 용도로 사용하고 있다.

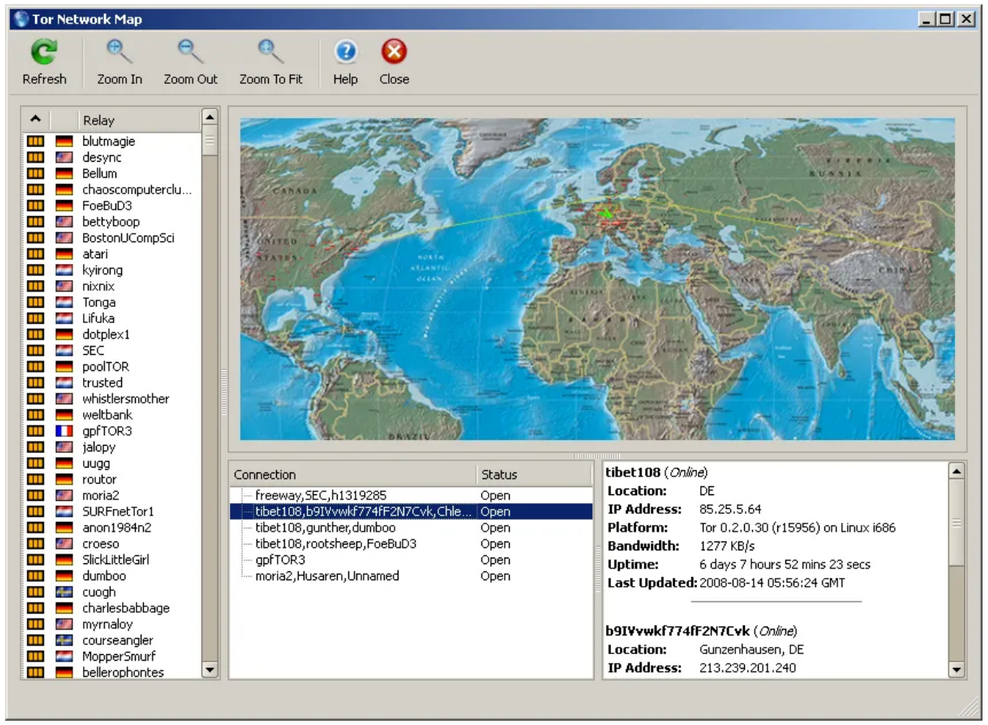
6. 동작 원리

일반적인 인터넷 통신은 사용자의 PC가 ISP를 통해서 목적지(서버, 또는 타 PC)에 연결해서 데이터를 주고 받는 식으로 이루어진다. 이 경우 트래픽을 전달하는 중계자(망)가 국가, 또는 준국가 기관이기 때문에 쉽게 검열(특정 사이트 차단)을 할 수 있고, 원칙상 대다수의 국가에서 불법이긴 하지만 원한다면 얼마든지 누가 누구에게 통신하고 있는지를 감청할 수 있다.



하지만 토어는 목적지까지 한 번에 통신하지 않고, 중간에 같은 토어 라우터를 실행하고 있는 노드들을 여러 개 거쳐서 보낸다. 즉 A→Z 가 아니라 A→B→C→D→Z 로 빙빙 돌려서 보내는 식이다. 토어가 일반 브라우저에 비해 느린 이유가 바로 이 때문이다.

이름(양파 라우터)처럼 패킷을 양파 껍질처럼 겹겹이 암호화해서 보내고, 이때 각각의 노드의 공개키를 통해 암호화하므로, 패킷의 출발지와 목적지를 알아내려면 거의 모든 노드를 장악해야 한다. 예를 들면 위의 예시에서 정부기관(또는 해커)이 C 노드를 장악했다고 해도, "B에서 왔음, D로 보내시오"라는 정보밖에 알 수 없다.[10]



설상가상으로 8900개의 노드가 전 세계에 흩어져 있으며[11], 일정 시간마다[12] 랜덤하게 hopping 노드들을 바꿔가며 통신하게 되어 있으므로, 전 세계의 tor 네트워크의 상당수의 노드들을 장악하지 않는 이상 tor를 이용한 통신은 추적이 힘들다.

어느 한 통신에서 entry/exit node로 사용되고 있는 노드가 장악당한 경우, 통신 속도를 이용해서 '바로 전 노드가 출발지다'/'바로 다음 노드가 도착지다'라는 것을 비교적 높은 확률로 추측할 수가 있**었**다. 하지만 이것도 통신 사이 사이에 랜덤하게 딜레이를 넣어주는 기능이 추가되어서 어렵게 되었다.

일반적인 프록시 우회방식과 다르게 프로그래밍된 DNS 패치 등을 사용해 3중 4중으로 보호되는데, 이 때문에 오직 토어 유저만 접속할 수 있는 일종의 인트라넷이 형성되어 있다. 해시암호.**onion**[13] 형식의 도메인을 쓰는데 일반적인 브라우저로는 표시되지 않는다. 이것을 우리는 흔하게 **다크웹**으로 부른다.

7. 보안 레벨과 브리지

토어 브라우저 설정에서 보안 레벨을 높이면 사용자를 사이버 상의 공격으로부터 보호하기 위해 브라우저의 기능이 일부 비활성화된다. 보안 레벨을 조정하여 언제든지 브라우저 기능을 다시 활성화할 수 있다.

- Standard

이 수준에서 모든 토어 브라우저 및 웹 사이트 기능이 활성화된다.

- Safer

HTTPS가 아닌 모든 사이트에서 JavaScript가 비활성화된다. 일부 글꼴 및 수학 기호 또한 비활성화된다. 오디오 및 비디오(HTML5 미디어)는 클릭해야 재생된다.

- Safest

모든 사이트에서 JavaScript가 비활성화된다. 일부 글꼴, 아이콘, 수학 기호 및 이미지 또한 비활성화된다. 오디오 및 비디오(HTML5 미디어)는 클릭해야 재생된다.

토어 네트워크에 대한 직접 액세스는 때때로 인터넷 서비스 제공업체나 정부에 의해 차단될 수 있다.(ex. 러시아, 중국) 토어 브라우저에는 이러한 검열을 우회하기 위해 브리지 기능이 있다. 보통 obfs4를 사용한다.

- obfs4

토어 트래픽을 무작위로 보이게 하여 검열을 우회한다.

- meek-azure

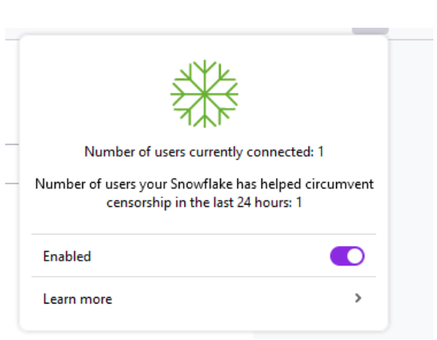
Microsoft 웹 사이트를 사용하는 것처럼 보이게 하여 검열을 우회한다.

7.1. Snowflake

Snowflake가 켜져있을 때 뜨는 아이콘	누군가가 자신의 Snowflake를 사용할 때 뜨는 아이콘

Snowflake는 토어까지도 차단당한 국가에서 토어를 이용할 수 있도록 개발된 토어의 브릿지이다.

기본적인 원리는 토어가 차단되지 않는 국가의 릴레이를 프록시 서버(엔드포인트)처럼 이용하여, 평범한 인터넷을 하는 것처럼 보이게 만들어, 토어의 이용이 불가능한 국가에서도 토어를 이용할 수 있게 만든다. 무엇보다 Snowflake 릴레이를 운영하는 것은 **브라우저 확장 프로그램에서 버튼 하나만 누르는 것이 가동의 전부**일 정도로 토어의 입구 노드, 출구 노드 운영에 비해 **훨씬 쉽고 리스크도 적어** 일반 유저들이 토어 네트워크에 기여할 때 이것을 사용하는 경우가 많다. 2022년부터 우크라-러시아 전쟁의 여파로 러시아의 인터넷 검열이 심해짐에 따라, 러시아에서 Snowflake 사용률이 매우 증가했다. 또한 2022년 이란 시위로부터 비롯된 이란의 인터넷 검열을 피하는 수단으로도 지목되어, 당시 페르시아어 가이드가 공개되기도 했다.



다음 링크는 🔗파이어폭스 브라우저 에드온, 🔗크롬(크로미엄 기반) 브라우저 에드온 이다.

8. 익명성

🔗필독: 토어 브라우저 설치/설정 방법🔗@

처음 사이트를 방문할 때 영문 사이트를 요청하겠냐는 질문이 나오면 반드시 영문 사이트 요청 버튼을 눌러야 익명성을 확보할 수 있다. 사이트에 한국어를 요청했다는 기록이 남기 때문이다. 놓쳤다면 설정에서 영문 사이트 요청하기를 키자. 참고로 표시 언어가 영어일 필요는 없다.

토어 네트워크는 주의사항만 준수한다면 NSA도 쉽게 추적할 수 없는 강력한 익명성을 보장한다. 때문에 인터넷 검열이 심한 국가에서 검열을 피하기 위한 용도부터 마약 및 총기 거래, 살인청부, 아동 포르노 제작, 유포 등이 이루어지는 불법적인 웹 사이트를 안전하게 운영하기 위한 용도까지 다양한 목적으로 이용되고 있다.

다만 2024년 9월 독일이 허니팟 노드를 이용해 타이밍 공격을 성공했다는 의혹이 나왔다. #

8.1. 사용 사례

- IP 차단 우회
  한국 IP를 차단하는 오덕 계열 사이트는 의외로 매우 많다. 여기 한국인 있어요 같은 이유로 차단한 경우가 많은데, 이러한 차단을 무력화하는 데 토어가 유용하다. 그래서 그런지 한국 유저가 전체의 3%로 전체 중 8위였으나 스마트폰 보급 이후 대체 서비스(VPN 등 IP 우회를 할 수 있는 프로그램)가 알려지면서 줄어들었다.
  하지만 토어 네트워크의 속도는 무료 프록시 서버나 VPN에 비해 느리니 속도만을 중시한다면 다른 수단을 이용하는 게 낫다. 토어 네트워크는 보안성과 익명성을 중시하기 위해 여러 국가의 중계 서버를 거치기 때문에 굉장히 느릴 수밖에 없는데(그래도 요새는 기술의 발달, 전 세계적으로 전체적인 네트워크 인프라가 상향되어 **1080p 60fps 유튜브 재생**[14][15]은 턱걸이가 가능하다. 당연히 광고도 다른 나라 것이 나온다.), 단순히 범죄성이 없는 지역 차단된 사이트 들어가자고 토어 같이 복잡한 구조를 거칠 필요는 없다. 이런 경우에는 VPN을 사용하자는 것.[16]

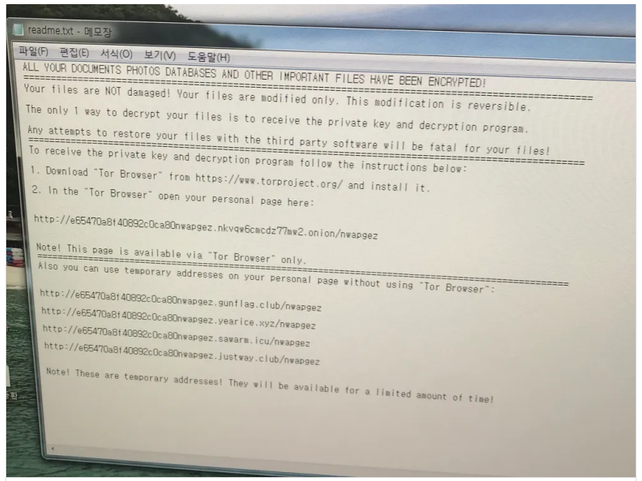
- 검열 우회[17]
  이걸로 검열을 피해 포르노 따위를 보려고 시도하는 경우도 있는데, 볼 수는 있겠지만 위에서 언급했듯이 VPN 등의 일반적인 우회수단보다 매우 느리므로 이쪽도 VPN을 알아보는 게 낫다.

- 언론, 표현의 자유
  이란 심리전의 일환으로 미국 정부에서 전폭적으로 밀어주고 있다고 한다. 실제로 인터넷 규제가 심한 이란에서의 토어 사용량은 세계 2위라고 한다. 넷상에서의 익명성을 중요하게 생각하는 Geek들이 여러 가지 실용적, 철학적인 이유로 토어를 애용하며, 정부나 기타 권력기관들과 대립 관계에 있는 인권 운동가들도 많이 사용한다. 2010년 브래들리 매닝 일병이 미군 기밀 자료를 위키리크스에 유출시킬 때도 토어와 다른 프로토콜을 사용했다고 한다. 에드워드 스노든도 Tails OS[18]에서 토어 네트워크를 이용하여 언론과 접촉했다. 중국에서 황금방패 우회를 위해 사용하기도 한다.[19]

- 군사/첩보 활동
  토어 공식 홈페이지에는 놀랍게도 군사목적으로서의 토어 사용에 대해서도 기술하고 있다. 다름 아닌 첩보 활동이라고 한다. 애초에 이 소프트웨어가 어디에서 만들어진 건지 생각해 보자. 실제로 CIA와 미국 국무부도 자체적으로 어니언 사이트를 운영하고 있으며 정보 제보자의 안전을 위해 Tor를 이용할 것을 권유하고 있다.

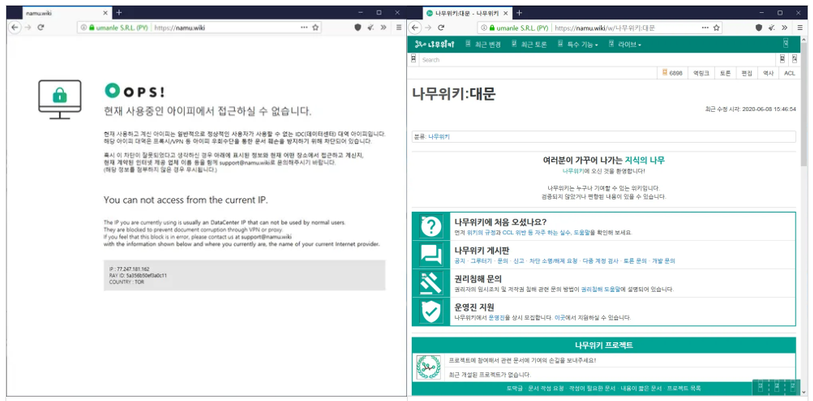
- 추적 우회
  IP가 드러나지 않으므로, IP 기반 추적을 방어할 수 있다. 채팅 사이트 등지에서 해커들이 링크 접속을 유도하여 IP를 확보하려 하는 경우가 있는데 토어 브라우저를 사용하면 아무리 의심스러운 링크라고 해도 그 링크로 접속한 사이트는 변조된 아이피로 접속되므로 아이피 위치 추적을 피할 수 있다. 이를 이용하여 자신에게 오는 스미싱 문자도 토어 브라우저로 접속할 시에는 신원정보 추적도 피할 수 있게 된다.

- 범죄
  범죄조직들도 토어를 사용한다. 왜냐면 토어의 기능 중 하나가 일반 웹 브라우저로는 접속할 수 없는 다크웹에 접속할 수 있기 때문. 마약, 살인청부, 아동 포르노, 불법 무기거래, 돈세탁, 악성코드 유통 등등의 중범죄까지 다양한 범죄 유형이 토어 네트워크 상에서 일어난다. 그리고 비트코인 같은 가상화폐와 결합해서 거래의 은폐도 가능해 상당한 문제가 되고 있다. 예를 들면 랜섬웨어 안내 주소에서 onion 도메인과 그 안에서 비트코인으로 돈을 내라고 협박한다.



랜섬웨어에 걸린 컴퓨터에서 보이는 안내문. 토어 브라우저를 다운로드하라고 적혀있다.

- 위키 반달



토어 접속이 차단된 경우

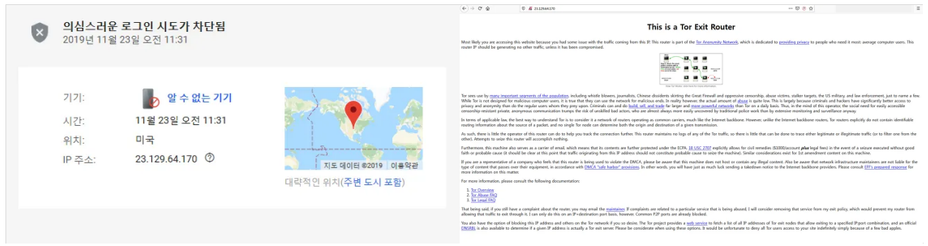
뚫린 경우. 간혹 문서 편집까지 뚫리기도 한다.

위키백과 등의 위키 사이트에서는 스팸이나 반달리즘을 방지할 목적으로 토어를 통해 접속한 사람 중 비회원의 문서 작성 및 편집을 철저히 제한한다. 당연히 가입한 회원의 경우 토어로 접속해도 위키백과 ⛓ 편집이 가능하다. 하지만 리그베다 위키에서는 토어를 사용한 편집을 막았으며 나무위키는 토어를 이용한 접속까지 막았으나[20] 토어 특성상 잘 뚫리는 편이다. 편집을 막는 이유는 수시로 변하는 IP 때문에 반달을 차단하는 게 쉽지 않기 때문이다. 토어로 접속하는 대다수 유저를 잠재적 반달로 간주하고 금지하는 것.

- 악플
  강한 익명성과 아이피를 우회하여 개인정보를 숨길 수 있다는 특성 때문에 고소를 회피하기 위해 비로그인 상태로 글 작성이 가능한 커뮤니티 사이트 전반에서 사용된다. 특히 유동 아이피로 인해 비로그인 작성이 활발한 디시인사이드 등지에서는 토어 사용자의 댓글에 어디 응디냐(어느 나라 IP냐)[21], 아스가르드에 사냐는 반응이 자주 달린다.[22][23]

- 암호화폐와의 콜라보레이션
  알다시피 비트코인은 생각보다 투명하게 운영되고 있다. 비트코인 지갑 소유주와 주인이 동일인임을 법적으로 증명하기는 힘들지만, 대한민국에서 빗썸(BITHUMB) 등의 거래소들은 죄다 실명 인증을 해야 거래가 가능하다. 하지만 문제는 비트코인은 현금 등으로도 거래가 가능하다는 점이다. 토어 네트워크를 이용한 비트코인 지갑을 활용하여 몇 번 코인 세탁을 해주면 법적으로 지갑 소유주와 당신이 동일인임을 증명할 수 없다. 이 과정에서 온라인 거래소를 이용하여 현금 인출하면 걸리지만, 팔 때도 현금으로 팔면 안 걸린다. 디지털 포렌식의 원칙 중 하나는 법처럼 **유죄임을 증명**해야 하는 건데 **심증만 있으므로** 처벌을 받지 않는다! 그 밖에도 토어를 이용한 비트코인 지갑 서비스를 운영하는 .onion 사이트들이 있으며, 이들은 비트코인 출금할 때 수수료를 조금 더 받음으로써 이익을 얻는다.

- 계정 해킹


의심스러운 로그인 시도가 차단됨
2019년 11월 23일 오전 11:31
기기: 알 수 없는 기기
시간: 11월 23일 오전 11:31
위치: 미국
IP 주소: 23.129.64.170
대략적인 위치(주변 도시 포함)
This is a Tor Exit Router

구글, 트위터, 페이스북 등의 계정들을 해킹하기 위해 사용되기도 한다. 위의 사진은 구글 로그인 시도이다.[24]

- C&C 서버
  악성 코드와 연결되는 서버(일종의 지령)를 IP로 바로 연결하면 추적될 수 있기에 백도어가 토어 네트워크를 거쳐 C&C 서버로 연결되도록 하는 경우도 존재한다. 이 경우에는 서버가 보호 대상이기에 사실상 플러그인이나 스크립트를 이용한 추적조차 불가능하다. 극악의 확률로 공격자가 이중 또는 삼중 토어를 사용하게 된다면 돌이킬 수 없다.

- 딥 웹, 히든 위키 이용
  히든 위키 문서를 보면 알겠지만 토어로만 접속 가능하고, 문서 상당수가 범죄와 관련되어 있다.

- 스팸
  Tor 네트워크에서 발생하는 주요문제로 많은 tor 출구노드는 스팸발신으로 쓰인다 그래서 tor 출구노드 호스팅을 AUP에서 허용하는 호스팅도 대부분 25, 465, 587등의 SMTP포트의 차단을 요구한다.

8.2. Operation Onymous

2014년 11월 6일경, 유로폴 측에서 미국과 유럽연합의 경찰 조직이 모여서 토어에서 운영되던 각종 마약 밀거래 및 청부 살인 사이트 등 총 410개의 불법 사이트를 차단했다고 ⛓ 밝혔다. 유로폴 측에서는 토어가 제공하는 익명성을 악용한 범죄 단체는 더 이상 도망칠 곳이 없다고 선언했지만 의례적으로 하는 말일 가능성이 매우 높다. 매우 특수한 경우에서 검거된 것이라는 게 정설이다. 게다가 사이트 운영자가 아닌 이용자는 아예 잡히지 않았다. 이에 대해 ⛓ 토어

프로젝트 블로그에서는 적발된 사이트의 보안이 허술하여 추적된 것으로 추측되지만, 토어 라우터 중 일부가 '물리적으로' 점거당하여 공격 대상이 노출되었을 가능성도 없지 않다고 밝혔다. 어느 쪽이든 특수한 상황이라는 것이다.

8.3. 악성 코드를 이용한 추적

FBI가 아동 포르노 사이트 서버를 압수한 뒤 여기에 '콘허스커'(Cornhusker, 강냉이 탈곡기)라는 악성코드를 심어놓고, 토어를 통해 접속자들의 컴퓨터를 감염시켜 익명성을 무력화한 후 IP를 수집하고 이들을 기소하는 사건이 벌어졌다. 기소자들은 사생활 침해 소송을 걸었지만 패소했다. 🔗 관련기사 저런 방식의 수사를 피하려면 독서실 등의 공용 네트워크를 이용하며 TMAC등으로 맥 어드레스까지 변조해야 한다.

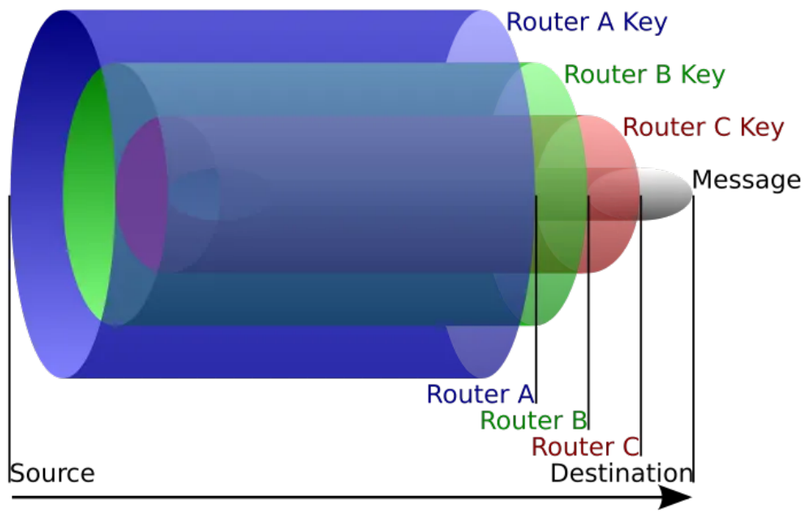
8.4. 국가의 검열

심층패킷검사(DPI)[25] 기술을 이용하면 토어를 원천 차단할 수 있다. DPI 기술은 원래 네트워크 조정에 쓰이는 기술이지만 이것을 악용하면 사용자의 인터넷상의 행적을 감시할 수 있다. 토어의 경우 통신하는 내용과 대상을 알 수 없다. 토어를 사용하는지 여부만을 알 수 있고, 그마저도 VPN을 사용하면 회피할 수 있다. 물론 이러면 VPN을 쓰고 있는 것으로 보이는데, 토어를 차단하는 국가라면 VPN도 수상하게 볼 확률이 높다. 때문에 정부에서는 이 기술을 통신사가 남용하지 않도록 엄격히 관리해야 함이 옳으나, 에티오피아 같은 경우에는 오히려 국가가 나서서 이 기술을 이용해 토어를 차단해버렸다. 🔗 기사 다만 요즘 토어 브라우저에서는 우회를 자동으로 해준다.

그게 아니라도 대놓고 국가차원에서 감청법을 만들고 패킷을 까 보는 것을 합법화하면 ISP 수준에서 무력화될 수밖에 없다. 황금방패나 홍콩보안법, 로스콤나조르 같이 DNS와 패킷을 까는 데는 장사 없다. 우편물이 익명성을 가질 수 있는 건 내용물을 굳이 열어보지 않기 때문이지, 국가가 모든 편지를 하나하나 까보겠다고 마음먹으면 아무리 중간에 여러 군데를 거치든 결국 들키는 것과 같다. 애초에 패킷 자체에 암호 복호키부터 어디를 거쳐서 최종적으로 어디로 가라고 다 써놓기 때문이다. 다만 현실적으로 표적수사가 아닌 이상 모든 개인의 패킷을 감청하는 건 양적으로 불가능하다.

8.5. 첫 노드와 끝 노드의 장악

토어 브라우저가 이용하는 중계서버(Relay)의 개수는 상당히 많지만 위의 Atlas나 Globe에서 볼 수 있듯이 이들은 **위치한 국가와 IP가 모두 알려졌다.**



물론 서버로 전달될 때까지 토어 네트워크의 노드 사이에서 계층적으로 공개키 암호화 방식을 사용하기 때문에, 첫 노드(A)에서 모든 트래픽을 감시[26]한다고 하여도 내 아이피가 무언가 보내고 있다는 것만 알 수 있을 뿐이지 B가 C에게, 또 최종적으로 C가 서버에게 무슨 내용을 주고 받는지 알 방법이 없다.[27] 이런 이유로 A의 입장에선 C의 아이피를 알 수 없다는 보안상의 장점도 존재한다.

하지만 암호화를 한다고 해도 패킷의 IP 자체는 숨기거나 할 수 있는 것이 아니기 때문에 이를 통해 출구 노드에서 거꾸로 물리적으로 장악해가게 되면 결국 토어 사용자의 IP에 도달하는 것이 가능은 하다. 다만 아직까지 출구 노드, 중간 노드, 입구 노드를 직접 따라가서 추적의 성공한 사례는 한번도 존재하지 않는다. 이는 토어를 VPN 서버를 여러 개 연결한 멀티홉 VPN쯤으로 착각하는 사람들이 주로 하는 생각으로 3개의 노드를 따라가면 되니 약간의 시간과 노력만 있으면 추적이 가능할 거라고 생각한다. 하지만 동일한 VPN 서버를 지속적으로 사용하고 VPN 서버 사이를 매번 암호화하고 복호화하는 멀티홉 VPN과 달리 토어는 매번 실행할 때마다 먼저 디렉토리 서버와 비대칭 암호화를 사용하여 연결된 후 8000개가 넘는 분산 해시 테이블로 연결된 노드중에 랜덤으로 3개의 노드를 선택한다. 그다음 어니언 라우팅으로 삼중 암호화되어 종단에 도달하기 직전까지 항상 암호화 상태를 유지하게 되며 노드들은 분산된 정보만을 얻을 수 있다 설령 노드에 문제가 있더라도 노드 구성이 10분주기로 자동으로 변경되기 때문에 실질적인 IP 추적의 효용성이 떨어진다. 이 때문에 토어의 익명성을 깨트리고 싶어하는 조직들은 대부분 토어 브라우저의 기반인 파이어폭스의 취약점으로 IP를 탈취하는 방식을 연구한다.

토어 프로젝트 자체적으로 악성 출구, 입구의 우려가 있을 경우에 badexit와 middleonly flag를 붙어서 중간 릴레이만 구동시키는 방식으로 대응한다.

2024년 9월 NDR의 기자가 프랑크프루트 검찰청에 2021년 다크웹 범죄자를 잡을 때 타이밍 분석을 사용했냐는 질문에 NCND로 답하여 독일이 수많은 허니팟 릴레이를 만들어[28] 범죄자에게 Ricochet[29]으로 채팅을 유도하고 타이밍 분석을 시행함으로써 Tor의 익명성을 훼손했다는 의혹을 받고 있다. 이에 대해 Tor Project 측은 Ricochet은 구형 onion 프로토콜을 쓰며 최신 프로토콜은 이런 공격이 막혀있다 말했다. 🔗 법 집행 기관이 토어 익명성을 훼손하는 방법(NDR) 🔗 Tor는 여전히 사용하기에 안전합니까?(Tor 프로젝트)

9. VPN과 병용

> Generally speaking, we don't recommend using a VPN with Tor unless you're an advanced user who knows how to configure both in a way that doesn't compromise your privacy.
> 일반적으로 말해서 개인 정보를 손상시키지 않는 방식으로 두 가지를 모두 구성하는 방법을 알고 있는 고급 사용자가 아니라면 Tor와 함께 VPN을 사용하지 않는 것이 좋습니다.
>
> 🔗 Can I use a VPN with Tor?
> The improper combination of Tor and another service may actually degrade a user's security and anonymity. These configurations are difficult to set up and should only be attempted by advanced users. For the vast majority of Whonix ™ users, using Tor in isolation - without a VPN or proxy - is the correct choice.
> Tor와 다른 서비스의 부적절한 조합은 실제로 사용자의 보안과 익명성을 저하시킬 수 있습니다. 이러한 구성은 설정하기 어려우며 고급 사용자만 시도해야 합니다. 대다수 Whonix™ 사용자의 경우 VPN이나 프록시 없이 Tor를 단독으로 사용하는 것이 올바른 선택입니다.
>
> 🔗 Combining Tunnels with Tor
> "보안상 위험하다는 게 아니라 잘못 설정 연결하면 위험할 수도 있으니 주의하고 쓰라는 거겠지"
> "보안상 위험보다는 정확하게 이해 못 하고 쓰는 새끼들이 존나 많으니까 걍 쓰지 말라고 하는 거 같음"
>
> 🔗 Tor와 VPN

아래 2가지 연결이 있다.

- 유저 → VPN → Tor → 인터넷
- 유저 → Tor → VPN → 인터넷
- VPN + Tor는 토어 단독 사용보다 무조건 좋다. (X)
- VPN + Tor를 할 경우 꼼꼼히 알아보고 해야 한다. (O)
- 일반적인 경우 토어 단독 사용이 올바른 선택이다. (O)

위의 내용을 보면 "아니, Tor과 VPN을 같이 사용하면 하나만 사용했을 때보다 더욱 안전한 거 아니었나?" 라는 의문점과 함께 "Tor과 VPN을 같이 사용하면 되레 보안상 치명적인 문제가 생기는 건가?" 할 수 있지만, 꼭 그렇지는 않고 아래 세 가지의 경우가 있다.

- Tor와 VPN을 같이 사용하는 것이 Tor만 단독 사용하는 거에 비해 별다른 이점이 없는 경우
- Tor와 VPN을 같이 사용했을 때 VPN이 Tor의 보호 모델을 깨뜨려 '완벽한 익명'에서 '덜 완벽한 익명'이 되는 경우
- Tor와 VPN을 병행 사용하는 것이 상황에 따라 Tor 단독 사용보다 더욱 나은 경우

2번째 케이스부터 먼저 설명하자면, 위에서 말한 '보안상 위협'과 '개인정보 손상'은 엄청 위험하고 거창해 보이지만 사실은 2번째 케이스에 해당한다. 즉 Tor와 VPN을 병행 사용하면 **문자 그대로 개인정보가 유출된다는 게 아니고**, 보안의 강도가 조금 느슨해진다는 뜻으로 받아들여야 정확하다.

3번째 케이스는 대부분의 사람에게 해당되는 것이자 또는 자신이 완전한 보안을 보장받길 원하여 VPN에 연결하고 Tor 브라우저를 킨 경우인데, 사실 '완전한'이라는 말 자체부터가 실현되긴 어렵지만 그래도 Tor 단독 사용보다는 Tor+VPN 병행 사용이 나을 때가 더 많다. 왜냐하면 병행 사용 시 VPN은 사용자가 Tor 브라우저를 켰다는 사실마저도 감추기 때문이다. 다만, NordVPN이나 Proton VPN 같은 오픈소스와 노로그를 감사받은 신뢰할 수 있는 VPN을 써야 한다. 그리고 VPN과 병행 사용하다 서버가 불안정해지면, 일부 사이트 요청이 통신사 DNS로 새어 나가게 되는데, 개인정보가 직접 새어나가는 건 아니지만 인터넷 제공업체가 사용자가 무엇을 했는지는 대충 어렴풋이 식별할 수 있다. 이렇게 되면 완전한 익명에서 덜 완전한 익명이 되어 2번째 케이스에 해당되게 된다.

1번째 케이스는 특정 운영체제나 특정 환경에서 해당되는데, 운영체제가 브라우저의 요청을 직접 컴파일하거나, 특정 브라우저 내장 VPN등을 사용하는 예외적인 케이스에서는 Tor 브라우저와 VPN을 같이 쓴다고 해서 딱히 보안상 이점이 생기지는 않는다. 오히려 속도만 이중으로 느려질 뿐이다.

다만 Tor 브라우저에서는 VPN 자체가 지문 추적에 취약하다는 등, 데이터가 다른 곳으로 새어 나갈 수 있다는 등의 주장을 펼치지만 이를 직접적으로 증명하는 근거는 없다. 설령 개인정보가 새어 나간다고 해도 VPN 그 자체에는 문제가 없을 수도 있다.

즉 요약하면, Tor와 VPN을 같이 사용하는 것은 보안상 이점이 분명히 존재하는 건 맞지만 항상 올바른 선택은 아니다. Tor 브라우저만 단독 사용하면 '사이트 요청이 새어나간다, 브라우저에 특정 패턴이 남는다' 같은 별다른 고민을 할 필요 없이 매우 높은 보안을 제공받을 수 있으므로 Tor 브라우저를 단독 사용하는 것이 권장되는 것이다.

10. 억압적인 국가에서의 검열 우회

이 문단의 내용 중 전체 또는 일부는 I2P 문서의 r158 판, 10번 문단에서 가져왔습니다. 이전 역사 보러 가기

> If I take your question as "What to do if I'm worried about getting caught running an I2P router in an oppressive regime," and you are worried about the authorities associating your computers with I2P traffic in the long term, and you still want to run an I2P router, then there are generally two solutions:
>
> - Run I2P off-site somewhere it is legal, and access it via an innocuous-seeming form of encrypted connection, such as an SSH connection or an HTTPS connection.
> - Encapsulate your I2P traffic in something legal. If a VPN is legal, then that I guess. If SSH is legal, an SSH tunnel.
>
> But, suppose your adversary is waiting for you to download a particular file that they know you are going to try and download anonymously. If they observe you downloading something that looks like a file of a similar size on your HTTPS tunnel or SSH tunnel or VPN, they're just going to assume that file is what they wanted to catch you with and come after you anyway.
> In fact, at the point where your adversary is willing to go after all I2P users, or all Tor users, or all bittorrent users or TLS users or bitcoin users or whatever, it's impossible to just give people "Settings" that can guarantee they will never be under suspicion. I mean, presumably you got an executable installer from https://i2p.net/, right? So you made DNS requests that say "I'm interested in I2P" you connected to the I2P web site and you downloaded a file about ~18.5 Mb in size. In such a draconian regime, you either get I2P from an unofficial channel, likely a sneakernet channel, or you are already under suspicion. Then you have to re-seed from a channel that can't be monitored easily as well, hopefully your sneakernet guy brought you a fresh reseed file to start with. You get the internet you use it on with a cantenna. You get the idea. In these kinds of very oppressive regimes, technology must be combined with planning, including possibly escape plans.
> Fortunately, only a few countries have this kind of law so far.
> 만약 당신의 질문을 "억압적인 정권 아래에서 I2P 라우터를 운영하다가 적발될까 봐 걱정된다면 어떻게 해야 할까요?"로 이해한다면, 그리고 당국이 당신의 컴퓨터를 I2P 트래픽과 장기적으로 연관시킬까 봐 걱정되지만, 그럼에도 불구하고 I2P 라우터를 운영하고 싶다면 일반적으로 두 가지 해결책이 있습니다.
>
> - I2P를 합법적인 외부 장소에서 운영하고, SSH 연결이나 HTTPS 연결처럼 무해해 보이는 암호화된 연결을 통해 접속하는 것입니다.
> - I2P 트래픽을 합법적인 방식으로 캡슐화하는 것입니다. VPN이 합법적이라면 VPN을 사용할 수 있고, SSH가 합법적이라면 SSH 터널을 사용할 수 있습니다.
>
> 하지만, 만약 당신의 적이 당신이 익명으로 다운로드하려는 특정 파일을 기다리고 있다고 가정해 봅시다. 만약 적이 당신이 HTTPS 터널이나 SSH 터널, 또는 VPN을 통해 비슷한 크기의 파일을 다운로드하는 것을 목격한다면, 그들은 그 파일이 당신이 익명으로 다운로드하려던 파일이라고 단정짓고 당신을 추적할 것입니다.
> 사실, 적이 모든 I2P 사용자, 모든 Tor 사용자, 모든 Bittorrent 사용자, TLS 사용자, 모든 Bitcoin 사용자 등을 표적으로 삼으려 한다면, 사람들이 절대 의심받지 않도록 보장하는 "설정"을 제공하는 것은 불가능합니다. 예를 들어, 여러분은 https://i2p.net/에서 실행 가능한 설치 프로그램을 다운로드했을 겁니다. 즉, "I2P에 관심이 있습니다"라는 DNS 요청을 보내고, I2P 웹사이트에 접속해서 약 18.5MB 크기의 파일을 다운로드했을 겁니다. 이렇게 엄격한 규제 체제에서는 비공식 채널, 아마도 Sneakernet 채널을 통해 I2P를 다운로드하거나, 아니면 이미 의심을 받는 상황에 놓이게 됩니다. 게다가 감시가 어려운 채널에서 시드 파일을 다시 제공해야 하는데, Sneakernet에서 제공한 파일이 처음부터 새것이기를 바라야겠죠. 인터넷 연결은 안테나 같은 걸로 합니다. 대충 어떤 상황인지 아시겠죠? 이처럼 억압적인 체제에서는 기술과 함께 탈출 계획을 포함한 철저한 준비가 필수적입니다.
> 다행히 현재까지 이러한 법을 제정한 나라는 극소수에 불과합니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

> To me, the safest way to run freenet in a hostile country is the following:
>
> - Know Freenet users either in countries with more relaxed laws or people who know people
> - Install freenet in a VM that's using full disk encryption OR on a VPS in another country. If remote node, connect to fproxy via SSH tunnel. Deleting a VM using full disk encryption takes seconds and is hard to recover valuable data from.
> - Connect with friends as darknet peers. Make sure they're not an informant. This is an opsec thing.
> - Use Freenet
>
> Never run your node in anything but high security, even once.

> 제 생각에 적대적인 국가에서 Freenet을 안전하게 운영하는 가장 좋은 방법은 다음과 같습니다.
>
> - 법이 비교적 완화된 국가의 Freenet 사용자 또는 그들을 아는 사람들을 통해 Freenet 사용자를 확보하세요.
> - 전체 디스크 암호화를 사용하는 가상 머신(VM) 또는 다른 국가의 VPS에 Freenet을 설치하세요. 원격 노드인 경우 SSH 터널을 통해 fproxy에 연결하세요. 전체 디스크 암호화(Full Disk Encryption)를 사용하는 VM은 삭제하는 데 몇 초밖에 걸리지 않으며 중요한 데이터를 복구하기 어렵습니다.
> - 친구들과 Darknet 피어로 연결하세요. 정보원이 아닌지 반드시 확인하세요. 이는 작전 보안과 관련된 사항입니다.
> - Freenet을 사용하세요.
>
> 노드를 실행할 때는 절대로 최고 수준의 보안 설정 외에는 다른 설정을 사용하지 마십시오. 단 한 번이라도 사용해서는 안 됩니다.
>
> https://www.reddit.com/r/Freenet/comments/bfh6oe/if_you_live_in_very_hostile_region_of_the_world/ @

> If you're going to be in a place where you're worried about that, your laptop will be searched on arrival, and fairly well. You will need to go further, and hide the application. Maybe even compile it once you arrive.
> Being caught with these things on your computer upon entrance to said country might land you in prison.
> 만약 그런 문제가 걱정되는 곳에 가신다면, 도착 시 노트북 검사를 꽤 꼼꼼하게 받게 될 겁니다. 더 나아가, 해당 애플리케이션을 숨겨야 할 수도 있습니다. 어쩌면 도착 후에 직접 컴파일해야 할지도 모릅니다.
> 해당 국가 입국 시 컴퓨터에 이런 것들이 있는 것이 적발되면 투옥될 수도 있습니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

https://www.whonix.org/wiki/Bridges

USER -(SSH)-> VPS -(Tor,I2P,Hyphanet,GNUnet)-> Website

신뢰할 수 있는 VPS에 **Tor**, I2P, Hyphanet, GNUnet 같은 프로그램을 설치하고 SSH로 터널링(Tunnelling)하여 ISP로부터 익명 네트워크 사용을 숨길 수 있다. ISP는 유저가 VPS와 SSH로 통신하고 있다는 사실만 알 수 있다. 단 이용하는 VPS를 신뢰해야 한다는 단점이 있다.

11. 국가별 릴레이

Tor Control Panel의 정보로 작성된 내용 개수를 동작하는 릴레이 기준으로 내림차순이다. 오로지 중간만 실행하는 릴레이도 있기 때문에 총 개수와 출구, 가드 릴레이를 합친 개수는 다르다

국가	가드	출구	동작하는 릴레이
독일	907개	439개	1638개
미국	724개	239개	1456개
네덜란드	346개	456개	766개
폴란드	233개	266개	335개
프랑스	222개	65개	330개
핀란드	166개	7개	248개
오스트리아	19개	110개	194개
영국	65개	10개	176개
캐나다	106개	16개	162개
루마니아	81개	104개	160개
스위스	85개	41개	151개
스웨덴	86개	49개	148개
룩셈부르크	120개	114개	138개
노르웨이	65개	49개	138개
이탈리아	31개	12개	73개
불가리아	48개	23개	72개
호주	7개	1개	60개
스페인	25개	-개	58개
몰도바	39개	10개	57개
러시아	38개	30개	58개
체코	28개	13개	54개
아이슬란드	28개	24개	52개
싱가포르	8개	5개	47개
덴마크	30개	16개	46개
우크라이나	25개	16개	45개
일본	12개	-개	37개
리투아니아	22개	1개	30개
헝가리	15개	5개	26개
브라질	6개	2개	22개
그리스	12개	1개	22개
유럽 연합	9개	1개	21개
라트비아	9개	1개	21개
벨기에	9개	1개	19개
대한민국	9개	1개	17개
튀르키예	10개	2개	17개
홍콩	3개	2개	16개
남아프리카 공화국	8개	4개	15개
아일랜드	7개	-개	15개
크로아티아	1개	10개	14개
포르투갈	7개	1개	13개
말레이시아	-개	1개	12개
인도네시아	-개	3개	11개
인도	3개	1개	11개
대만	1개	1개	11개

멕시코	3개	1개	10개
세르비아	2개	-개	10개
슬로바키아	3개	-개	9개
뉴질랜드	4개	1개	8개
이스라엘	2개	1개	8개
베트남	-개	3개	7개
태국	-개	1개	6개
코스타리카	3개	3개	6개
세이셸	4개	5개	6개
카자흐스탄	2개	1개	5개
칠레	1개	2개	5개
슬로베니아	2개	1개	4개
키프로스	1개	-개	3개
알바니아	3개	-개	3개
아랍에미리트	1개	1개	2개
아르헨티나	-개	-개	2개
우즈베키스탄	-개	=개	2개
필리핀	-개	-개	2개
아르메니아	=개	1개	1개
페루	1개	1개	1개
아제르바이잔	1개	-개	1개
안도라	-개	-개	1개
레위니옹	-개	-개	1개
지브롤터	1개	1개	1개
방글라데시	-개	-개	1개
푸에르토리코	-개	-개	1개
모리셔스	-개	-개	1개
키르기스스탄	=개	-개	1개

12. 검열 국가

- torproject.org 도메인 접근을 차단하는 나라[30]
  - 러시아
    - Roskomnadzor의 HTTP 무응답 정책
  - 미얀마
    - DPI·SNI·도메인·IP기반 차단과 국지적 셧다운의 병행
  - 바레인
    - DNS·URL·IP 필터
  - 벨라루스
    - 의도적 연결 지연
  - 사우디아라비아
    - DNS 차단
  - 아랍에미리트
    - 패킷 차단
  - 예멘
    - DNS 차단
  - 오만
    - 상위망 라우팅과 중앙화된 카테고리 필터
  - 우즈베키스탄
    - 의도적 연결 지연
  - 이란
    - QUIC·TLS 무응답
  - 이집트
    - 의도적 트래픽 지연
  - 중국
    - DNS 차단과 IP·SNI 기반 패킷 드롭
  - 카타르
    - 프록시 기반 URL·도메인 필터
  - 쿠웨이트
    - ISP의 URL·IP 차단

13. 악용에 대한 프로젝트의 입장

원문

> Q. Doesn't Tor enable criminals to do bad things?
>
> A. Criminals can already do bad things. Since they're willing to break laws, they already have lots of options available that provide better privacy than Tor provides. They can steal cell phones, use them, and throw them in a ditch; they can crack into computers in Korea or Brazil and use them to launch abusive activities; they can use spyware, viruses, and other techniques to take control of literally millions of Windows machines around the world.
> Tor aims to provide protection for ordinary people who want to follow the law. Only criminals have privacy right now, and we need to fix that.
> Some advocates of anonymity explain that it's just a tradeoff — accepting the bad uses for the good ones — but there's more to it than that. Criminals and other bad people have the motivation to learn how to get good anonymity, and many have the motivation to pay well to achieve it. Being able to steal and reuse the identities of innocent victims (identity theft) makes it even easier. Normal people, on the other hand, don't have the time or money to spend figuring out how to get privacy online. This is the worst of all possible worlds.
> So yes, criminals can use Tor, but they already have better options, and it seems unlikely that taking Tor away from the world will stop them from doing their bad things. At the same time, Tor and other privacy measures can fight identity theft, physical crimes like stalking, and so on.
>
> Q. 토어는 범죄자가 나쁜 일을 할 수 있게 하지 않습니까?
>
> A. 범죄자들은 이미 나쁜 짓을 할 수 있습니다. 그들은 기꺼이 법을 위반하기 때문에 토어가 제공하는 것보다 더 나은 개인 정보 보호를 제공하는 많은 옵션을 이미 가지고 있습니다. 그들은 휴대폰을 훔쳐서 사용하고 도랑

에 던질 수 있습니다. 그들은 한국이나 브라질의 컴퓨터에 침입하여 악의적인 활동을 시작하는 데 사용할 수 있습니다. 스파이웨어, 바이러스 및 기타 기술을 사용하여 문자 그대로 전 세계 수백만 대의 Windows 시스템을 제어할 수 있습니다.
토어는 법을 준수하고자 하는 일반 사람들을 보호하는 것을 목표로 합니다. 지금은 범죄자들만이 사생활을 가지고 있고 우리는 그것을 고쳐야 합니다.
익명성을 옹호하는 일부 사람들은 나쁜 용도를 좋은 용도로 받아들이는 것은 단지 절충안일 뿐이라고 설명하지만 그 이상의 의미가 있습니다. 범죄자 및 기타 나쁜 사람들은 좋은 익명성을 얻는 방법을 배우려는 동기가 있으며 많은 사람들이 이를 달성하기 위해 많은 비용을 지불하려는 동기를 가지고 있습니다. 무고한 피해자의 신원을 도용하고 재사용(신원 도용)할 수 있다는 점은 이를 더욱 쉽게 만듭니다. 반면에 일반 사람들은 온라인에서 개인 정보를 보호하는 방법을 알아내는 데 사용할 시간이나 돈이 없습니다. 이것은 모든 가능한 세계 중 최악입니다.
예, 범죄자는 토어를 사용할 수 있지만 이미 더 나은 옵션이 있으며 토어를 세상에서 제거한다고 해서 그들이 나쁜 일을 하는 것을 막을 수는 없을 것 같습니다. 동시에 토어 및 기타 개인 정보 보호 조치는 신원 도용, 스토킹과 같은 물리적 범죄 등과 싸울 수 있습니다.

Q. Where does Tor Project stand on abusers using technology?

A. We take abuse seriously. Activists and law enforcement use Tor to investigate abuse and help support survivors. We work with them to help them understand how Tor can help their work. In some cases, technological mistakes are being made and we help to correct them. Because some people in survivors' communities embrace stigma instead of compassion, seeking support from fellow victims requires privacy-preserving technology.
Our refusal to build backdoors and censorship into Tor is not because of a lack of concern. We refuse to weaken Tor because it would harm efforts to combat child abuse and human trafficking in the physical world, while removing safe spaces for victims online. Meanwhile, criminals would still have access to botnets, stolen phones, hacked hosting accounts, the postal system, couriers, corrupt officials, and whatever technology emerges to trade content. They are early adopters of technology. In the face of this, it is dangerous for policymakers to assume that blocking and filtering is sufficient. We are more interested in helping efforts to halt and prevent child abuse than helping politicians score points with constituents by hiding it. The role of corruption is especially troubling; see this United Nations report on The Role of Corruption in Trafficking in Persons.
Finally, it is important to consider the world that children will encounter as adults when enacting policy in their name. Will they thank us if they are unable to voice their opinions safely as adults? What if they are trying to expose a failure of the state to protect other children?

Q. 토어 프로젝트는 기술을 사용하는 남용자에 대해 어떤 입장이십니까?

A. 우리는 남용을 심각하게 생각합니다. 활동가와 법 집행 기관은 토어를 사용하여 학대를 조사하고 생존자를 지원합니다. 우리는 그들과 협력하여 그들이 토어가 그들의 작업을 어떻게 도울 수 있는지 이해하도록 돕습니다. 경우에 따라 기술적 실수가 발생하고 있으며 이를 수정하는 데 도움을 줍니다. 생존자 커뮤니티의 일부 사람들은 연민 대신 낙인을 받아들이기 때문에 동료 피해자의 지원을 구하려면 개인 정보 보호 기술이 필요합니다.
우리가 토어에 백도어 구축과 검열을 거부하는 것은 우려가 부족해서가 아닙니다. 우리는 토어를 약화시키는 것을 거부합니다. 토어를 약화시키는 것은 물리적 세계에서 아동 학대와 인신매매를 퇴치하려는 노력에 해를 끼치고 온라인에서 피해자를 위한 안전한 공간을 제거하기 때문입니다. 한편, 범죄자들은 여전히 봇넷, 도난당한 전화, 해킹된 호스팅 계정, 우편 시스템, 특사, 부패한 공무원 및 콘텐츠 거래를 위해 등장하는 모든 기술에 액세스할 수 있습니다. 그들은 기술의 얼리어답터입니다. 이에 직면하여 정책 입안자들이 차단 및 필터링으로 충분하다고 가정하는 것은 위험합니다. 우리는 정치인들이 아동 학대를 숨기도록 돕는 것보다 실제로 아동 학대를 중단 및 예방하는 것에 더 관심이 있습니다. 특히 부패는 아동 학대와 인신매매 문제를 해결하는데 골칫거리입니다. 그에 관해서는 인신매매에서 부패의 역할에 관한 이 UN 보고서를 참조해 주십시오.
마지막으로 아이들의 이름으로 정책을 추진할 때 아이들이 어른이 되어 마주하게 될 세상을 고려하는 것이 중요합니다. 아이들이 어른이 되었을때 안전하게 자신의 의견을 말할 수 없다면 과연 우리에게 고마워할까요? 국가가 아이들을 보호하는 것에 실패했을 때 그들이 폭로하지 못하게 되어 버리면 어떻게 해야 합니까?

토어를 악용하는 사람들 때문에 토어에 대해 부정적인 인식이 있다. 심지어 토어 사용을 금지해야 한다고 주장하는 사람도 있다. 그러나 토어는 검열로부터 우리를 보호해 주고, 내부고발 이후 보복으로부터 지켜 줄 수 있다. 토어를 금지시킨다면 토어 사용이 자유로웠던 때보다 표현의 자유가 억눌리게 되는 것은 분명하다.

14. 관련 문서

- 다크 웹
- I2P
- Hyphanet(구 Freenet)
- GNUnet
- 가상 사설망
- Tails OS
- Whonix
- Mullvad Browser
- Check It Onion
- OONI - Tor Project에서 분리된 프로젝트

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.